Notice of Allowability	Application No.	Applicant(s)	
	09/603,636	FUTA, YUICHI	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6 June 2005*.

2. ☒ The allowed claim(s) is/are *2,4-10,12-18,20-24,26 and 28-32*.

3. ☒ The drawings filed on *26 June 2000* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

In the claims:

Claim 17, Line 12, replace "equations Ax=b, the equation solving means including" with –equations Ax=b,--

Claim 26, Line 40, replace "before the transformationin each transformation" with –before the transformation in each transformation"

Allowable Subject Matter

2. Claims 2, 4-10, 12-18, 20-24, 26 and 28-32 are allowed.

3. The following is an examiner's statement of reasons for allowance: Applicant's claimed invention discloses an apparatus and method comprising a machine readable memory that provides instructions for solving a system of linear equations Ax=b in n

unknowns on a finite field GF(p), where p is prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements. The prior art of record, Curtis Linear Algebra: An introductory approach and Shamir USPN 5,375,170 suggest a similar invention; however neither Curtis nor Shamir teaches or suggests the following limitations of independent claim 1:

a. generating the coefficient matrix C and the constant vector d of the system of linear equations Cx=d from the coefficient matrix W and the constant vector b of the system of linear equations Ax=b includes one or more successive transformation processes;

b. the system of linear equations Ax=b is subjected to the first transformation process and the system of linear equations Cx=d is generated as a result of the last transformation process;

c. in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

d. in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

e. each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and

f. in each transformation subprocess,

i. each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values generated as a result of the multiplications are set into a second coefficient group,

ii. each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and

iii. the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

4. In addition, neither Curtis nor Shamir teach or suggest the following limitations of independent claim 6:

g. generating the coefficient matrix C and the constant vector d of the system of linear equations Cx=d from the coefficient matrix W and the constant vector b

of the system of linear equations Ax=b includes one or more successive transformation processes;

h. the system of linear equations Ax=b is subjected to the first transformation process and the system of linear equations Cx=d is generated as a result of the last transformation process;

i. in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

j. in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

k. each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

l. in the coefficient group calculation process,

iv. a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of

the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a firtt coefficient group, and

v. each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equation, and values generated as a result of the multiplications are set into a second coefficient group; and

m. in each transformation subprocess for transforming a separate one of the one or more object equations,

vi. a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to 0 as a new coefficient,

vii. each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the Second coefficient group calculated from the coefficients in the pivotal equation are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients; an

viii. a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the object equation to generate a difference, and the constant in the object equation is changed to the difference as a new constant.

5. In addition, neither Curtis nor Shamir teach or suggest the following limitations of independent claim 9:

n. computing an inverse 1 of an element y in GF(q) which is an extension field of a finite field GF(p), where p is a prime, q=p^n, and n is a positive integer, the apparatus comprising:

ix. equation generating means for generating a coefficient matrix W and a constant vector b for a system of linear equations Ax=b in n unknowns, using the element y and all coefficients of a generator polynomial of GF(q) whose root is @,

x. equation solving means for finding solutions xk (k=0, 1, 2, ..., n-1) of the system of linear equations Ax=b,

xi. inverse computing means for computing the inverse I, I=x0 + x(I)@ + ... + x(n-I)@^(n-I), using the root @ and the solutions xk (k=0, 1, 2, ..., n-I) found by the equation solving means.

6. In addition, neither Curtis nor Shamir teach or suggest the following limitations of independent claim 17:

o. record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over GF(q) as a basis for security and recorded on a record medium, an inverse I of an element y in GF(q) to decrypt the encrypted digital content recorded on the record medium, where GF(q) is an extension field of a finite field GF(p), p is a prime, q=p^n, n is a positive integer, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

xii. equation generating means for generating a coefficient matrix W and a constant vector b for a system of linear equations Ax=b in n unknowns, using the element y and all coefficients of a generator polynomial of GF(q) whose root is @,

xiii. equation solving means for finding solutions xk (k=0, 1, 2, ... n-1) of the system of linear equations Ax=b;

xiv. inverse computing means for computing the inverse I, I=x0 + x(I)@ + ... + x(n-I)@^(n-I), using the root @ and the solutions xk (k=0, 1, 2, ..., n-I) found by the equation solving means; and

xv. means for using I to decrypt the encrypted digital content recorded on the record medium.

7. In addition, neither Curtis nor Shamir teach or suggest the following limitations of independent claim 26:

p. generating the coefficient matrix C and the constant vector d of the system of linear equations Cx=d from the coefficient matrix W and the constant vector b of the system of linear equations Ax=b includes one or more successive transformation processes;

q. the system of linear equations Ax=b is subjected to the first transformation process and

r. the system of linear equations Cx=d is generated as a result of the last transformation process,

s. in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation in each transformation process, one pivotal equation which is a linear equation in a unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

t. each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and

u. in each transformation subprocess,

xvi. each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values generated as a result of the multiplications are set into a second coefficient group,

xvii. each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and

xviii. the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

8. In addition, neither Curtis nor Shamir teach or suggest the following limitations of independent claim 30:

v. generating the coefficient matrix C and the constant vector d of the system of linear equations Cx=d from the coefficient matrix, A and the constant vector b of the system of linear equations Ax=b includes one or more successive transformation processes;

w. the system of linear equations Ax=b is subjected to the first transformation process and the system of linear equations Cx=d is generated as a result of the last transformation process;

x. in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

y. in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

z. each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

aa. in the coefficient group calculation process,

xix. a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a first coefficient group, and

xx. each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equations, and values generated as a result of the multiplications are set into a second coefficient group; and

bb. in each transformation subprocess for transforming a separate one of the one or more object equations,

xxi. a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to 0 as a new coefficient,

xxii. each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the second coefficient group calculated from the coefficients in the pivotal equations are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients, and

xxiii. a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the

object equation to generate a difference, and the constant in the object equation is changed to the difference as a new constant.

For these reasons, claims 2, 4-10, 12-18, 20-24, 26 and 28-32 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
June 16, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100